EX 29 :

1. a/ B→i=2⇒ $a^i=5^2=25\equiv 3(11)$ ⇒f(i)=3→C
   A→i=1⇒ $a^i=5^1=5\equiv 5(11)$ ⇒f(i)=5→E
   C→i=3⇒ $a^i=5^3=125\equiv 4(11)$ ⇒f(i)=4→D

Message	B	A	C
i	2	1	3
f(i)	3	5	4
Code	C	E	D

b/ F→i=6⇒ $a^i=5^6\equiv 5\ (11)$ ⇒f(i)=5→E
A→i=1⇒ $a^i=5^1=5\equiv 5(11)$ ⇒f(i)=5→E
D→i=4⇒ $a^i=5^4\equiv 9(11)$ ⇒f(i)=9→I
E→i=5⇒ $a^i=5^5\equiv 1\ (11)$ ⇒f(i)=1→A

Donc le message «FADE» est codé «EEIA»

On ne peut pas déchiffrer avec certitude le message codé car E peut-être déchiffrer F ou A.

2. a=2

Message	A	B	C	D	E	F	G	H	I	J
i	1	2	3	4	5	6	7	8	9	10
f(i)	2	4	8	5	10	9	7	3	6	1
Code	B	D	H	E	J	I	G	C	F	A

Oui on peut déchiffrer avec certitude un message codé (bijection)

3. a/ (⇒)

$a^{i'}\equiv a^i(11)\Leftrightarrow a^{i'}=a^i+11k\Leftrightarrow a^{i'}-a^i=11k\Leftrightarrow a^i.(a^{i'-i}-1)=11k$

$$\Rightarrow \left.\begin{array}{l} 11\left|a^i(a^{i'-i}-1)\right. \\ or\ 11\wedge a=1 \end{array}\right)\Rightarrow 11\left|a^{i'-i}-1\right.\Rightarrow a^{i'-i}\equiv 1(11)$$

(⇐) si $a^{i'-i}\equiv 1(11)\Rightarrow a^{i'-i}.a^i\equiv 1.a^i(11)\Rightarrow$

Cl :

$$\boxed{a^{i'}\equiv a^i(11)\quad\Leftrightarrow\quad a^{i'-i}\equiv 1(11)}$$

b/ f permet de chiffrer et de déchiffrer avec certitude tous les messages ssi $\forall i'\neq i\ \ a^{i'}\neq a^i(11)$ ssi $a^{i'-i}\neq 1(11)$ i et i' deux entiers compris entre 1 et 10 et i<i'

$\Rightarrow i'-i\in\{1,2,3,\ldots,9\}$

ssi a^i n'est pas congru à 1 modulo 11 pour tout $i\in\{1,2,3,\ldots,9\}$

c/ On a a< 11 donc 11 ne divise pas a ;et comme 11 nombre premier Alors d'après th de Fermat $a^{10}\equiv 1(11)$

Supposons que k ne divise pas 10 alors 10= n.k+u avec u<k

$a^k\equiv 1(11)\Rightarrow a^{n.k}\equiv 1(11)$ et comme $a^{10}\equiv 1(11)$ Alors $a^{10-n.k}\equiv 1(11)\Rightarrow a^u\equiv 1(11)$ avec u<k

Absurde car k est le plus petit entier deΩ tel que $a^k\equiv 1(11)$.

d/ Pour bien choisir a il suffit que a^2 et a^5 ne sont pas congrus à 1 modulo 10.

Qarray.tn -Aqra Blech- Qarray.tn